Priorités d'analyse

Publié: 2023-09-19

Le système ExtraHop analyse le trafic et collecte les données de tous les dispositifs découverts sur un seul capteur. Chaque appareil découvert reçoit un niveau d'analyse qui détermine les données et les métriques collectées pour un appareil. Les priorités d'analyse déterminent le niveau d'analyse d'un appareil.

Important: Les priorités d'analyse peuvent être gérées de manière centralisée à partir d'une console.

Niveaux d'analyse

Chaque appareil reçoit l'un des niveaux d'analyse suivants.

Note: Les enregistrements et les paquets sont disponibles pour tous les périphériques des systèmes ExtraHop configurés avec un recordstore ou un packetstore, quel que soit le niveau d'analyse.

Mode découverte

Le système ExtraHop identifie les matériels et logiciels connus, les utilisateurs authentifiés et les adresses IP attribuées et associées. Le système ExtraHop génère également des détections et des graphiques qui montrent l'activité du protocole observée sur l'appareil. Tous les appareils reçoivent au minimum ce niveau d'analyse, à l'exception des appareils parents L2.

Analyse standard

Le système ExtraHop inclut au moins une semaine de métriques L2-L3 et de données sur les relations avec les pairs que vous pouvez explorer instantanément par le biais de détections, de graphiques et de cartes d'activité. Le système ExtraHop identifie également le matériel et les logiciels connus des appareils, les utilisateurs authentifiés et les adresses IP attribuées et associées. Apprenez à prioriser les groupes pour l'analyse standard.

Analyse avancée

Le système ExtraHop inclut au moins une semaine de métriques L2-L7 provenant de plus de 50 protocoles et de données sur les relations entre pairs que vous pouvez instantanément explorer par le biais de détections, de graphiques et de cartes d'activité, ainsi que de tableaux de bord, de rapports et d'alertes personnalisés. Le système ExtraHop identifie également le matériel et les logiciels connus, les utilisateurs authentifiés et les adresses IP assignées et associées. Apprenez à prioriser les groupes pour l'analyse avancée ou à ajouter un appareil individuel à une liste de surveillance.

Analyse des parents L2

L'analyse parentale L2 n'est applicable que si la découverte L3 est activée sur le système ExtraHop. À l'exception des passerelles et des routeurs, les périphériques parents L2 reçoivent automatiquement ce niveau d'analyse, qui collecte les métriques de protocole L2-L3 et les cartes d'activité.

Analyse des flux

Un capteur de flux collecte des données à partir de journaux de flux, au lieu de paquets, pour analyse par le système ExtraHop. Les appareils découverts sur des capteurs de flux reçoivent automatiquement ce niveau d'analyse. Les paramètres du système Priorités d'analyse ne sont pas disponibles pour les capteurs de flux, et les périphériques en analyse de flux ne peuvent pas être ajoutés à la liste de surveillance.

Voir le tableau comparant ces niveaux d'analyse.

Hiérarchisation des appareils et des groupes

Le système ExtraHop peut analyser des centaines de milliers de périphériques et déterminer automatiquement le niveau d'analyse de chacun d'entre eux, mais vous pouvez contrôler quels périphériques sont prioritaires pour l'analyse avancée et l'analyse standard.

La plupart des appareils peuvent être ajoutés à une liste de surveillance pour garantir une analyse avancée, ou vous pouvez ajouter des groupes d'appareils à une liste ordonnée pour les classer par ordre de priorité pour l'analyse avancée et l'analyse standard.

Voici quelques considérations importantes concernant la hiérarchisation des dispositifs par le biais de la liste de surveillance :

- Les appareils restent dans la liste de surveillance même s'ils sont inactifs, mais les mesures ne sont pas collectées pour les appareils inactifs.
- Le nombre d'appareils dans la liste de surveillance ne peut pas dépasser votre capacité d'analyse avancée.
- Les appareils ne peuvent être ajoutés à la liste de surveillance qu'à partir de la page des propriétés d'un appareil ou de la page de la liste des appareils. Vous ne pouvez pas ajouter de dispositifs à la liste de surveillance à partir de la page Priorités d'analyse.
- Si vous souhaitez ajouter plusieurs dispositifs à la liste de surveillance, nous vous recommandons de créer un groupe de dispositifs, puis de donner la priorité à ce groupe pour l'analyse avancée.
- Les dispositifs qui reçoivent l'analyse des parents L2 ou l'analyse des flux ne peuvent pas être ajoutés à la liste de surveillance.

Voici quelques considérations importantes concernant la hiérarchisation des groupes de périphériques :

- Ordonnez les groupes de dispositifs de la priorité la plus élevée à la priorité la plus faible dans la liste.
- Cliquez et faites glisser les groupes pour modifier leur ordre dans la liste.
- Assurez-vous que chaque appareil du groupe est actif ; les groupes contenant un grand nombre d'appareils occupent de la capacité et les appareils inactifs ne génèrent pas de métriques.
- Vous ne pouvez pas hiérarchiser plus de 200 groupes de dispositifs pour chaque niveau.

Par défaut, le système ExtraHop remplit automatiquement les niveaux d'analyse avancé et standard jusqu'à leur capacité maximale. Voici quelques considérations importantes concernant les niveaux de capacité et l'option de remplissage automatique :

- Les appareils prioritaires dans la liste de surveillance ou par le biais d'un groupe prioritaire remplissent d'abord les niveaux d'analyse supérieurs, puis les appareils découverts le plus tôt.
- Les dispositifs sont prioritaires pour l'analyse avancée s'ils sont associés à certaines détections, s'ils ont accepté ou initié une connexion externe ou s'ils utilisent des outils d'attaque courants.
- Les propriétés du dispositif, telles que le rôle, le matériel et le logiciel, l'activité du protocole, l'historique des détections et la valeur élevée, peuvent également déterminer les niveaux d'analyse.
- L'option Remplir automatiquement est activée par défaut. Si elle est désactivée, tous les périphériques qui ne font pas partie des groupes prioritaires ou de la liste de surveillance sont supprimés et le système ExtraHop définit la priorité pour chaque périphérique.
- Votre abonnement et votre licence ExtraHop déterminent les niveaux de capacité maximum.

Consultez le site FAQ sur les priorités d'analyse pour en savoir plus sur les capacités des niveaux d'analyse.

Comparer les niveaux d'analyse

Niveau d'analyse	Caractéristiques	Comment recevoir ce niveau
Mode découverte	• Détections • Protocoles observés	Les appareils reçoivent automatiquement le mode

Niveau d'analyse	Caractéristiques	Comment recevoir ce niveau
	• Adresses IP • Utilisateurs authentifiés • Logiciels • Marque et modèle du matériel	découverte s'ils ne sont pas en analyse standard, avancée ou parentale L2.
Analyse standard	• Métriques L2-L3 • Cartes d'activité • Détections • Protocoles observés • Adresses IP • Utilisateurs authentifiés • Logiciels • Marque et modèle du matériel	Prioriser les groupes de dispositifs pour l'analyse standard.
Analyse avancée	• Métriques L2-L7 • Métriques personnalisées • Cartes d'activité • Détections • Protocoles observés • Adresses IP • Utilisateurs authentifiés • Logiciels • Marque et modèle du matériel	Priorisez les groupes de périphériques pour l'analyse avancée ou ajoutez des périphériques individuels à la liste de surveillance.
Analyse parentale L2 (applicable uniquement si la découverte L3 est activée)	• Métriques L2-L3 • Cartes d'activité	Les périphériques parents L2 reçoivent automatiquement l'analyse parentale L2, à l'exception des passerelles et des routeurs.
Analyse des flux	• Métriques L2-L3 • Cartes d'activité • Protocoles observés • Adresse IP • Propriétés de l'instance de cloud • Types de détection limités	Les appareils reçoivent automatiquement une analyse de flux s'ils sont découverts sur un capteur de flux.